The present invention relates to a system for receiving broadcast digital data comprising a master digital terminal, and at least one slave digital terminal connected to the master terminal.

The market for digital television decoders is currently reaching a turning point. Most subscribers, in the European Countries in particular, are equipped with a single digital terminal (or « decoder ») per household, whereas they often possess at least two television sets. There therefore exists a demand for multiple equipment in terms of decoders for one and the same householdCertain operators of pay digital television wish to offer their subscribers the possibility of equipping themselves with several digital terminals so as to benefit from their services on each of the television sets installed in their accommodation, without however making them pay the price of a full tariff subscription for the additional terminals, which would be prohibited, but rather a reduced tariff (or even a zero tariff). However, the operator has to ensure that the terminals and « associated » subscriptions actually remain within the same household, since in the converse case, their income is at risk of being considerably affected thereby.

A known solution consists in using the « return path » of the digital terminals by requesting the subscriber to link all the terminals of his home to one and the same telephone line. The operator then periodically monitors the connection of the terminals to this telephone line by remotely instructing telephone calls from the terminals to a server of the operator. However, this solution is not satisfactory since it entails the permanent connection of the digital terminals of the subscriber to a telephone line.

Another solution described in French Patent Application No. 02 09362 filed on 24 July 2002 by the same applicant as the present application, THOMSON Licensing S.A., consists in guaranteeing that a physical communication link always exists between a secondary terminal (or « slave » terminal) and a main terminal (or « master » terminal) with which it is paired. The slave terminal or terminals (for which the subscriber benefits from a preferential tariff) cannot operate, that is to say provide data in clear to the television set to which they are connected without verification of the presence of the « master » terminal with which they are paired in proximity.

Several strategies for communication between these decoders are conceivable but some of them may exhibit risks of « piracy » or of « circumvention ».

The aim of the present invention is to afford an improvement to the invention described in the aforesaid patent application by minimizing the risks of piracy or of circumvention.

The principle of the invention is as follows: a « master » digital terminal contains a smart card in which are recorded entitlements paid for by the subscriber at the normal tariff. A « slave » digital terminal contains a smart card whose entitlements, identical or otherwise to those of the smart card of the « master » decoder, have been paid for more cheaply by the same subscriber.

This preferential tariff of the subscription of the « slave » decoder is granted by the operator on condition that the slave decoder is used by the same subscriber in the same accommodation as the « master » decoder.

The basic idea from which the invention stems consists in considering that if the « slave » digital terminal is not in immediate proximity to the « master » digital terminal, it is being used in a different accommodation and hence the subscriber is violating the contract allowing him to benefit from a preferential tariff. By virtue of the present invention, if such a situation of fraudulent use of the « slave » digital terminal is detected, the latter ceases to operate normally ; in this instance, it no longer allows the subscriber to access all the services that he is supposed to receive (picture and sound).

It will be noted that the invention may be implemented between a master digital terminal and several slaves, if the operator so permits.

The subject of the invention is a system for receiving broadcast digital data comprising a master digital terminal, and at least one slave digital terminal connected to the master terminal by a link and able to receive protected digital data. According to the invention, the slave digital terminal can access the protected data only if information necessary for accessing said data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline.

The protected digital data are in particular television services scrambled by keys and the information for accessing the protected data is in particular messages containing access entitlements to the services or else parameters making it possible to extract from such messages data received or else messages containing a part of the access entitlements.

According to a particular characteristic of the invention, the information received by the master digital terminal is transformed before being sent to the slave digital terminal. In particular, the information received by the master digital terminal is received from the broadcasting system in an encrypted

form and is decrypted in the master terminal before being sent to the slave terminal.

To summarize, the basic mechanism of the invention is as follows:

- the master digital terminal receives a part of the elements necessary for the descrambling of the services by the slave digital terminal ;
- these elements are sent to the slave digital terminal under conditions that are well defined and in a unique manner by way of a physical communication link between the two terminals;
- if the master digital terminal is not able to provide these elements to the slave digital terminal within a predetermined deadline, the slave digital terminal is not capable of accessing the service received.

The advantages of the invention are as follows: since it is based on security elements of the broadcasting system itself (the information exchanged between the terminals is encrypted with secrets managed by the data broadcasting system and by the smart cards of the digital terminals), the risk of piracy at the level of the smart card or of the digital terminal is reduced.

Moreover, since the invention relies on the "real time" aspect of the implementation, this eliminates the risk of prolongation of the physical link between two digital terminals by telephone or Internet network. Specifically, the physical link between the two digital terminals master and slave could be "lengthened" indefinitely by an Internet link: the service operator would then no longer have the guarantee that the two terminals are in the same household of a subscriber. By imposing, according to the principle of the invention, a maximum deadline for the transferring of the data, one thus ensures that the information does not travel via an Internet type link.

Another advantage of the invention is that it guarantees that each exchange of data is different from the previous one, and hence unpredictable. Specially, a pirate could be tempted to spy on the information which is received by the terminals so as to emulate the information expected on the part of the master digital terminal by the slave digital terminal with the aid of a pirate device (a computer for example). Since the information that is exchanged between the terminals changes with each communication, it is unpredictable and cannot therefore be easily emulated by a pirate device.

The invention will be better understood on reading the detailed description which follows of several embodiments. This description is given merely by way of example and refers to the appended drawings in which :

Figure 1 represents a schematic diagram of a system according to the invention.

Figure 2 illustrates a first embodiment of the invention.

Figure 3 illustrates a second embodiment of the invention.

Figure 4 illustrates a third embodiment of the invention.

Figure 5 illustrates a variant of the second embodiment.

Figure 6 illustrates a fourth embodiment.

In Figure 1, we have represented two digital terminals (or decoders): a master terminal 1 and a slave terminal 2, which are connected by a communication link 3. The two terminals receive, by way of a satellite antenna 4, digital data broadcast by a service operator, in particular audio/video data. They each comprise a smart card 15 / 25 in which are stored entitlements of the subscriber to access the services of the operator.

The data received are scrambled, according to the conventional principle of pay digital television, by scrambling keys (often called « control words ») and the keys are themselves encrypted and sent in messages labeled ECMs (the acronym standing for « Entitlement Control Message ») with the service related data. Personalized messages, labeled EMMs (standing for « Entitlement Management Message ») make it possible to update on each smart card each subscriber's « entitlement » (these entitlements may also be received via a subscriber telephone line to which the terminal is connected, as in the case of pay per view for example). To descramble a service to which a subscriber is entitled, the ECMs are dispatched to the smart card which provides the corresponding decrypted descrambling keys, these keys making it possible to descramble the service. The descrambling keys are dynamic and change every 10 seconds at most (« key period »).

The scrambled digital data are received by a tuner/demodulator 10 / 20 in each terminal 1 / 2. A demultiplexer and filtering device 11 / 21 extracts from the data received the ECMs and EMMs messages which are directed to the access control module 14 / 24. This module 14 / 24 decrypts the descrambling keys so as to send them to a descrambler 12 / 22, which receives the audio/video data A/V from the demultiplexing and filtering module 11 / 21. By virtue of the descrambling keys received from the module 14 / 24, the descrambler can descramble the A/V data and send them to a decoder, in particular an MPEG decoder 13 / 23 that outputs audio/video signals in clear for a television set.

According to the invention, a module for managing the pairing application 17 / 27 is present in the master terminal 1 and in the slave 2. It manages the communications between the two terminals and in particular the transferring of the information from the master terminal to the slave terminal so as to allow the slave terminal to access the data received. This module also controls the deadline that passes before the receipt of this information in such a way as to block the operation of the slave terminal if the information is not received within the fixed deadline. A communication port 16 / 26 disposed in each terminal manages the link between the two terminals.

Figure 2 illustrates a first embodiment of the invention, based on the EMMs.

It consists in providing the entitlements (EMMs) of the slave digital terminal by way of the master digital terminal and of the pairing communication link, rather than via the satellite antenna. In practice, the slave digital terminal 2 receives by satellite an EMM « EMM (End_of_entitlements) » that erases all or part of the entitlements of his smart card 25. Immediately afterwards, it receives an item of information « Message (Request_entitlements_from_master) » that it has to send to the master terminal 1 via the physical link 3. The master digital terminal uses this item of information to pick up an EMM sent slightly later. This EMM « Message (Slave_Entitlements) » is then immediately sent back to the slave digital terminal via the communication link 3. This EMM « Message (Slave_Entitlements) » allows the slave terminal 2 to update its entitlements in its smart card.

If the response from the master terminal 1 is not received within a due deadline (maximum deadline Δt), the slave decoder is blocked, until the next sending of EMMs.

It will be noted that the frequency of sending of the EMMs may be small (one or more days). Moreover, the maximum due deadline Δt should be long enough for the digital terminals to have time to process the information and short enough for a delay introduced by an intermediary of Internet Network type to be prohibitive and to block the slave terminal.

Figure 3 illustrates a second embodiment of the invention, likewise based on the EMMs.

It consists in providing the slave digital terminal 2 with the filtering information for the EMMs by way of the master terminal 1 and of the pairing communication link 3.

The slave terminal receives an EMM « EMM (Deletion_of_entitlements) » that cancels all or part of the entitlements of its card 25. Immediately after, the master terminal receives and this time sends back a message containing the filtering parameters of the EMMs « Message (Slave EMM filtering info) » of the slave terminal, this information having to be dispatched to the slave terminal via the communication link 3 within a given time.

The entitlements are then broadcast by the services operator to the slave terminal to which, by virtue of the information received from the master can pick up the EMM containing the entitlements of the « slave » card 25 and continue to operate normally.

If the slave digital terminal 2 has not received the EMM filtering information in time, the entitlements are not restored, and the slave terminal 2 no longer operates normally.

Other simple variants may be envisaged: for example the master terminal receives a part of the EMM (resp. ECM) from the slave terminal and sends it back to the slave terminal within a limited time span.

The implementations described hereinabove involve certain constraints of usage of the master terminal: it must be active and able to receive the EMMs/ECMs/messages permanently, on the one hand since the broadcast of the information by the broadcasting system is not predictable over time and on the other hand because the broadcasting system has no return of information regarding the fact that these EMMs/ECMs/messages have been received by their intended recipients.

The following implementation illustrated by Figure 4 makes it possible to reduce these constraints.

According to this embodiment of the invention, all or part of the entitlements of the slave terminal 2 are received in the form of an EMM and stored by the master terminal 1. The slave terminal 2 will request the master terminal for update of its entitlements at a later moment.

The time at which the exchange of information occurs may be chosen in such a way as to guarantee that this exchange will be successful (for example just after having verified that the communication between the two decoders is operational and/or making sure of the presence of the subscriber near his slave terminal so that he can follow any instructions). The operation must however take place during a limited time interval (for example a few days)

after the arrival of the EMMs, else the software module 27 of the slave terminal cancels the entitlements of its smart card 25.

The appropriate moment having come, the slave terminal 2 requests the EMM information from the master terminal 1, which must return this information within a maximum deadline of a few tens of milliseconds. If the information is not received within this deadline, the software module 27 of the slave terminal cancels the entitlements of its smart card 25.

The following implementation which is illustrated by Figure 5 makes it possible to reduce a risk related to the possible emulation of the messages dispatched by the master terminal to the slave terminal by an exterior device.

The information that is provided to the slave terminal is extracted from the stream broadcast by the broadcasting system by the master terminal. In the first two implementations, the information received by the master terminal 1 must be transferred to the slave terminal 2 immediately after receipt. A pirate device could be tempted to discover a correlation between the message flowing over the communication link 3 and the content of the broadcast transport stream received by the master terminal in previous instants, and thus be capable of reproducing the scheme for processing the transport stream so as to generate an identical message for the slave terminal within a sufficiently short deadline. This device could be either a computer equipped with a tuner/demodulator/demultiplexer, or the equivalent of another decoder together with suitable software, and be placed in proximity to the slave terminal, far from the master terminal.

To prevent it being possible to find such a correlation, the information received by the master digital terminal 1 must be transformed, according to this preferred implementation of the invention, before being dispatched to the slave terminal 2. The safest means available in a digital terminal for performing this transformation is the use of the DVB descrambler.

In practice, it is therefore a matter of dispatching to the master terminal 1 a special ECM, that is transformed, in the master smart card 15, into a descrambling key. The message containing the information for the slave terminal is then dispatched to the master terminal in data packets scrambled with this same key. Once descrambled, the packets may be processed by the master terminal to generate the message destined for the slave terminal.

This method is applicable to all the variant embodiments cited above. In Figure 5 it is applied to the second embodiment of the invention.

Figure 6 illustrates another variant embodiment making it possible to deal with another risk. This risk identified in particular for the third type of implementation is that of the emulation by an external device of the messages dispatched by the slave terminal to the master terminal to retrieve the EMM stored in the master terminal.

An external device connected to the master terminal could thus emulate the request of the slave terminal and intercept the response of the master terminal. This response could then be dispatched by the Internet to another external device linked to the slave terminal, that could then provide the right information when the slave terminal requests it.

To prevent such emulation, it is possible to propose either the use of a protocol secured with authentication, or more simply to use once again the resources of the smart card and of the broadcasting system.

The broadcasting system may in fact dispatch at a given moment to the master terminal and to the slave terminal a special ECM, which is transformed, in the master smart card into a descrambling key. Then the broadcasting system dispatches to each of the terminals an identical message (secret code), encrypted with these previously received keys. The messages containing the secret code are decrypted on each decoder by the smart card. The slave terminal 2 then tests the decrypted secret code. The master terminal waits for this message for a limited time span. If it receives it on time, it verifies that it is indeed the expected secret code by comparing it with that which it has itself received, then responds by dispatching the EMM to the slave terminal. If it does not receive the expected message in time, it does not dispatch the EMM information. Once its message has been dispatched, the slave terminal likewise waits for the response of the master for a limited time span. If the EMM information does not arrive within the due deadlines, the slave terminal does not update the entitlements of its smart card.

Such a device therefore makes it possible, on the one hand to render the exchange of information unpredictable, and on the other hand imposes the real-time constraint that prevents potential circumvention by Internet.